(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 15 680 A 1**

(51) Int. Cl.[6]:
H 04 L 9/12
H 04 L 9/16

(21) Aktenzeichen: 195 15 680.3
(22) Anmeldetag: 28. 4. 95
(43) Offenlegungstag: 31. 10. 96

DE 195 15 680 A 1

(71) Anmelder:
Alcatel SEL AG, 70435 Stuttgart, DE

(74) Vertreter:
Pohl, H., Dipl.-Ing., Pat.-Ass., 70435 Stuttgart

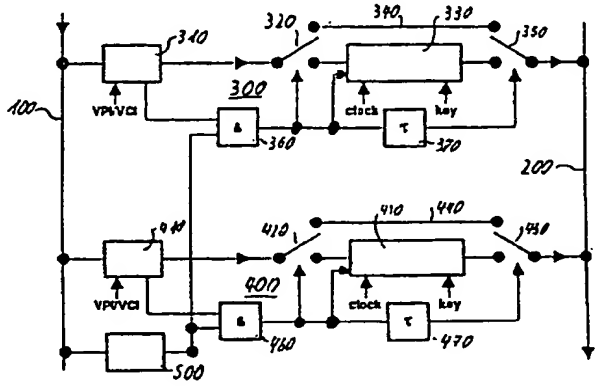
(72) Erfinder:
Böttle, Dietrich, Dipl.-Ing., 73084 Salach, DE;
Banniza, Thomas-Rolf, Dipl.-Ing., 71282 Hemmingen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

GB	21 68 573 A
US	52 68 962
US	49 10 777
US	47 39 510
US	43 16 055
EP	0 26 458 A3
EP	0 26 458 A2

(54) Verfahren zum Verschlüsseln und Entschlüsseln eines paketierten Nachrichtenstroms, sowie Verschlüssler und Entschlüssler dafür

(57) Technisches Problem:
Verschlüsselte Übertragung von ATM-Datenströmen.
Stand der Technik:
Verschlüsselungstechniken zur Ver- und Entschlüsselung beliebiger Datenformate.
Grundgedanke:
Suche im Datenstrom den Paketkopf derjenigen Pakete, die zu der zu ver- oder entschlüsselnden Nachricht gehören und ver- oder entschlüssele ausschließlich den hierzu gehörigen Nachrichteninhalt.
Beispiel:
Zeit- oder Raummultiplexanordnung für Ver- oder Entschlüsselung mehrerer Nachrichtenströme desselben Datenstroms.



DE 195 15 680 A 1

Beschreibung

Die vorliegende Erfindung betrifft ein Verfahren zum Verschlüsseln und Entschlüsseln eines Nachrichtenstroms, der in Form von Nachrichtenpaketen übertragen wird, nach dem Oberbegriff des Anspruchs 1, sowie einen Verschlüßler und einen Entschlüßler hierfür, nach dem Oberbegriff des Anspruchs 7 bzw. 8.

Geheimschriften, Verschlüsselungen und Entschlüsselungen sind so alt wie die Schrift. Auch für moderne Kommunikationsformen sind Verschlüsselungs- und Entschlüsselungstechniken bekannt. Diese kann man auch auf Nachrichten anwenden, die dann in Form von Nachrichtenpaketen übertragen werden. Die derzeit wichtigste Technik der Übertragung mit Datenpaketen ist der Asynchronous Transfer Mode (ATM), bei dem die Nachrichtenpakete als Zellen bezeichnet werden. Während es problemlos ist, die bekannten Techniken zur Verschlüsselung und Entschlüsselung auf noch zu paketierende Nachrichten anzuwenden, ist die Anwendung auf bereits paketierte, also schon in Form von Nachrichtenpaketen oder Zellen vorliegende Nachrichten problematisch.

Hier schafft die Erfindung Abhilfe durch ein Verfahren nach der Lehre des Anspruchs 1, sowie Verschlüßler und Entschlüßler nach der Lehre der Ansprüche 7 bzw. 8.

Die Paket- oder Zellköpfe, auch Header genannt, bleiben dabei grundsätzlich unverschlüsselt. Sie werden dazu verwendet, im Datenstrom diejenigen Pakete zu erkennen, die zu demjenigen Nachrichtenstrom gehören, der zu verschlüsseln oder zu entschlüsseln ist. Außerdem werden die Paketköpfe dazu verwendet, die entsprechenden Vorgänge mit dem Datenstrom zu synchronisieren.

Vorteilhafte Ausgestaltungen der Erfindung sind den Unteransprüchen zu entnehmen.

Ein ATM-Datenstrom wird in der Regel Zellen (Datenpakete) enthalten, die unterschiedlichen Nachrichtenströmen angehören. Soll der gesamte Datenstrom, zum Beispiel im Verlauf einer Richtfunkverbindung verschlüsselt übertragen werden, so kann dies nach herkömmlichen Verfahren erfolgen. Ist dagegen, zum Beispiel in einem Verteilnetz, der gesamte Datenstrom einer Vielzahl von Teilnehmern zugänglich, von denen jeder auf den ihn betreffenden Nachrichtenstrom zugreifen kann, so muß jeder dieser Nachrichtenströme für sich mit einem eigenen Schlüssel verschlüsselt übertragen werden. Der jeweilige Schlüssel kann dann aus dem unverschlüsselt übertragenen Paketkopf ermittelt werden. In einen solchen Datenstrom können natürlich auch Nachrichtenströme eingebettet sein, die sich an alle wenden, zum Beispiel Rundfunk oder Fernsehen, oder die aus sonstigen Gründen keiner Vertraulichkeit bedürfen. Diese können auch unverschlüsselt bleiben.

Für die Verschlüsselung der den Paketköpfen folgenden Nachrichtenteile selbst können die für kontinuierliche oder für in sich geschlossene Nachrichten bekannten Verfahren verwendet werden.

Eine bekannte Möglichkeit der Verschlüsselung ist die Blockkodierung, bei der die zu verschlüsselnden Daten in Blöcke aufgeteilt und jeder Block für sich als Ganzes mittels einer Abbildungsvorschrift auf einen anderen Block abgebildet wird. Eine besonders einfache Aufteilung ergibt sich, wenn jeder einem Paketkopf folgende Nachrichtenteil als solcher Block behandelt wird und wenn die Abbildungsvorschrift so ausgebildet ist, daß ein Block vor und nach der Abbildung gleich lang ist.

Bei der Blockkodierung hängt die Sicherheit gegen unbefugtes Entschlüsseln von der Länge und der Anzahl der verschlüsselt übertragenen Blöcke ab. Im vorliegenden Fall ist die Länge der Blöcke vorgegeben. Einer der derzeit untersuchten Anwendungsfälle ist das Abonnements-Fernsehen, wo die Länge der Übertragung gleich der Gültigkeitsdauer des Abonnements und die Anzahl der übertragenen Blöcke beliebig groß ist. Außerdem ist gerade hier der Anreiz zum unbefugten Entschlüsseln sehr hoch. Eine Abhilfemöglichkeit ist hier der häufige Wechsel der Schlüssel, das heißt der Abbildungsvorschrift. Wie dies auf gesicherte Weise erfolgen kann, ist nicht Gegenstand der vorliegenden Erfindung.

Eine andere Möglichkeit besteht in der Anwendung längerer Schlüssel. Hierfür bietet sich dann aber nicht mehr die Blockkodierung, sondern die Stromkodierung an. Dabei wird ein fortlaufender Datenstrom derart durch einen Algorithmus behandelt, daß sich daraus ein neuer Datenstrom ergibt, in dem aufeinanderfolgende Bits des einen Datenstroms auch aufeinanderfolgenden Bits des anderen Datenstroms entsprechen. Ein einfaches Beispiel besteht darin, sowohl den zu verschlüsselnden Datenstrom wie den zu entschlüsselnden durch eine Exklusiv-Oder-Funktion mit einer als Schlüssel dienenden Bitfolge zu verknüpfen. Eine "1" des Schlüssels läßt dabei das entsprechende Bit des Datenstroms unverändert, eine "0" dagegen invertiert diese. Sowohl das zweimalige aufeinanderfolgende Invertieren wie auch die zweimalige unveränderte Weitergabe ergibt im Ergebnis die ursprüngliche unverschlüsselte Bitfolge. Der Schlüssel kann dabei beliebig lang und damit beliebig sicher sein. Die Handhabung wird dabei aber schwieriger. Ein nicht zu langer gelegentlich gewechselter Schlüssel wird auch hier angebracht sein.

Bei dieser Art der Verschlüsselung, bei der über die Grenzen eines einem Paketkopf folgenden Nachrichtenteils hinweg verschlüsselt oder entschlüsselt wird, muß der Vorgang des Verschlüsselns bzw. Entschlüsselns am Ende eines Nachrichtenteils unterbrochen werden, bis der Anfang des nächsten zur selben Verbindung gehörigen Nachrichtenteils vorliegt.

Hier ergibt sich auch das Problem, die Vorgänge des Verschlüsselns und des Entschlüsselns aufeinander zu synchronisieren, vor allem die Synchronisation im Verlauf einer Übertragung zu überprüfen. Es gibt Anwendungen, wo im Paketkopf die Pakete einer Verbindung durchnumeriert sind. Diese Numerierung kann unter Umständen zur Synchronisation der Ver- und Entschlüsselung mit herangezogen werden.

Ist keine solche Numerierung vorhanden oder eine solche zum Zwecke der Synchronisation nicht geeignet, so werden in den zu verschlüsselnden Datenstrom geeignete Synchronisationswörter eingefügt.

Die der Synchronisation der Entschlüsselung dienenden Synchronisationswörter müssen vor der Entschlüsselung schon erkannt werden können, weil sie Voraussetzung für die Entschlüsselung sind. Sie dürfen deshalb nicht mit verschlüsselt werden. Auch laufende Nummern, die der Durchnumerierung der Pakete dienen, sind möglicherweise von der Verschlüsselung auszunehmen, wenn im Laufe der Übermittlung auf sie zugegriffen werden soll. Gleiches gilt auch für alle anderen Nachrichtenteile, die in irgendeiner Weise der Sicherung der Übertragung dienen. Sie werden damit letztlich dem Paketkopf zugeordnet

Im folgenden wird die Erfindung anhand eines Ausführungsbeispiels unter Zuhilfenahme der bei liegenden

Zeichnungen weiter erläutert.

Fig. 1 zeigt ein erstes Ausführungsbeispiel eines erfindungsgemäßen Verschlüßlers.

Fig. 2 zeigt ein zweites Ausführungsbeispiel eines erfindungsgemäßen Verschlüßlers.

Fig. 3 zeigt ein Ausführungsbeispiel eines erfindungsgemäßen Entschlüßlers.

Der Verschlüßler nach Fig. 1 weist eine Eingangsleitung 100, eine Ausgangsleitung 200, ein erstes und ein zweites Verschlüsselungsteil 300 bzw. 400 und ein Synchronisationsteil 500 auf.

Die beiden Verschlüsselungsteile sind untereinander gleich aufgebaut. Jedes Verschlüsselungsteil ist zur Verschlüsselung eines Nachrichtenstroms vorgesehen. Die Zahl von gerade zwei Verschlüsselungsteilen ist deshalb nur sehr symbolisch zu sehen. In der Regel werden mehrere Verschlüsselungsteile vorhanden sein. Aber auch Verschlüßler mit nur einem Verschlüsselungsteil können sinnvoll sein.

Jedes Verschlüsselungsteil weist ein Filter 310 bzw. 410, einen ersten Umschalter 320 bzw. 420, einen Verwürfler 330 bzw. 430, eine Umwegleitung 340 bzw. 440, einen zweiten Umschalter 350 bzw. 450, ein Und-Gatter 360 bzw. 460 und ein Verzögerungsglied 370 bzw. 470 auf.

Der auf der Eingangsleitung 100 ankommende Datenstrom wird den Filtern 310 und 410 und dem Synchronisationsteil 500 zugeführt. Jedem Filter ist die Kennung eines Nachrichtenstroms zugewiesen. Sie wird hier als VPI/VCI bezeichnet und kennzeichnet den virtuellen Pfad (virtual path identifier) und den virtuellen Kanal (virtual channel identifier), die diesem Nachrichtenstrom zugewiesen sind. Jedes Filter läßt nur die Pakete des zugehörigen Nachrichtenstroms passieren und meldet dies gleichzeitig dem zugehörigen Und-Gatter.

Das Synchronisationsteil 500 leitet aus dem ankommenden Datenstrom eine Maske ab, die diejenigen Teile des Datenstroms, die verschlüsselt werden dürfen, gegenüber den anderen maskiert. Diese Maske wird allen Verschlüsselungsteilen über deren Und-Gatter angeboten. Ob dann tatsächlich etwas verschlüsselt wird, hängt davon ab, ob das entsprechende Filter überhaupt eine Nachricht passieren läßt.

Der Ausgang des Und-Gatters 360 schaltet den ersten Umschalter 320, aktiviert den Verwürfler 330 und schaltet, über das Verzögerungsglied 370, den zweiten Umschalter 350. Dem Verwürfler 330 wird weiter ein Takt clock und ein Schlüssel key zugeführt. Die zu verschlüsselnden Teile des Nachrichtenstroms werden über den Umschalter 320, den Verwürfler 330 und den Umschalter 350 der Ausgangsleitung 200 zugeführt. Die nicht zu verschlüsselnden Teile werden mittels der beiden Umschalter 320 und 350 und der Umwegleitung 340 am Verwürfler vorbeigeleitet.

Das zweite Verschlüsselungsteil 400 arbeitet genauso, ebenso jedes etwaige weitere. Die jeweilige Kennung VPI/VCI und der jeweilige Schlüssel key werden im Zuge eines Verbindungsaufbaus eingestellt. Der Schlüssel key kann während der Verbindung ausgetauscht werden. Einstellung von Kennung und Schlüssel und etwaiger Schlüssel-Tausch erfolgen wie die Einstellung und Änderung anderer Parameter einer Verbindung. Dies ist nicht Gegenstand der vorliegenden Erfindung. Für bestimmte Fälle könnten auch unveränderliche und fest eingestellte Parameter verwendet werden.

Die Verwendung eines Verwürflers erfolgt hier nur beispielhaft. Hier kann jede Einrichtung verwendet werden, die einen passenden Verschlüsselungsmechanismus realisiert. Die Verzögerung des Verzögerungsglieds 370 muß, ebenso wie die Laufzeit der Umwegleitung 340, der Verarbeitungszeit im Verwürfler angepaßt sein.

Sofern der verwendete Schlüssel und die Paketanfänge nicht zueinander synchron sind, muß noch in geeigneter Weise eine zusätzliche Synchronisation im Verwürfler erfolgen. Inwieweit das Synchronisationsteil dabei in den Verwürfler hineinwirkt, hängt von der jeweils verwendeten Verschlüsselungsart ab. Dies ist insoweit nicht erfindungspezifisch.

Sind im Datenstrom auf der Eingangsleitung 100 noch weitere Datenpakete enthalten, etwa Steuerpakete oder Leerpakete, so müssen diese mittels eines weiteren Filters mit der entsprechenden Verzögerung zur Ausgangsleitung 200 durchgeschaltet werden.

Der Verschlüßler nach Fig. 2 ist ähnlich aufgebaut wie der nach Fig. 1. Zwischen der Eingangsleitung 100 und der Ausgangsleitung 200 liegt hier ein Verschlüsselungsteil 600 und das Synchronisationsteil 500.

Das Verschlüsselungsteil 600 weist in diesem Beispiel außer einem Filter 610, einem ersten Umschalter 620, einem Verwürfler 630, einer Umwegleitung 640, einem zweiten Umschalter 650 und einem Verzögerungsglied 670 noch ein weiteres Verzögerungsglied 680 und eine Schlüsselliste 690 auf.

Der Aufbau und auch die Wirkungsweise ist weitgehend gleich wie im vorigen Beispiel, jedoch wird hier ein Verschlüsselungsteil im Zeitmultiplex für die Verschlüsselung mehrerer Nachrichtenströme verwendet.

Das Filter 610 filtert hier die Paketköpfe soweit aus dem Datenstrom aus, wie dies zum Bestimmen des jeweils erforderlichen Schlüssels erforderlich ist. Die Paketköpfe werden aber auch im normalen Datenstrom weiter mitgeführt. Die aus den Paketköpfen ausgefilterten Informationen dienen der Adressierung der Schlüsselliste 690, die jeweils den richtigen Schlüssel an den Verwürfler 630 liefert. Die Eintragung der Schlüssel in die Schlüsselliste erfolgt nach Art der Einstellung eines Verbindungsparameters nach bekannten Verfahren. Für Steuer- und Leerpakete wie auch für nicht zu verschlüsselnde Nachrichtenströme kann ein Schlüssel eingetragen sein, der im Verwürfler keine Veränderung der Nachricht bewirkt.

Das weitere Verzögerungsglied 680 gleicht gegenüber dem Beispiel nach Fig. 1 die Verzögerung des Filters und des Und-Glieds aus.

Der Entschlüßler 700 nach Fig. 3 weist eine Eingangsleitung 720, ein Filter 710, einen Entwürfler 730, eine Ausgangsleitung 740 und ein Synchronisationsteil 500 auf.

Das Filter 710 blendet einen einzigen Nachrichtenstrom aus dem Datenstrom auf der Eingangsleitung 720 aus und führt ihn dem Entwürfler 730 zu, der mit demselben Schlüssel key die Wirkung des zugehörigen Verwürflers wieder aufhebt.

Im gezeigten Beispiel wurde unterstellt, daß am Ausgang des Entschlüßlers nur noch der reine Nachrichtenstrom benötigt wird. Das Filter 710 läßt deshalb in diesem Fall nur die Nachrichtenteile der ausgewählten Pakete durch. Eine Umleitung der Paketköpfe um den Entwürfler ist deshalb nicht erforderlich. Das Synchronisationsteil 500 dient hier ausschließlich der Synchronisation und nicht auch der Maskierung. Eine Umwandlung der ausgeblendeten Nachrichtenteile in einen kontinuierlichen Datenstrom wird hier nicht weiter beschrieben.

Patentansprüche

1. Verfahren zum Verschlüsseln und Entschlüsseln eines Nachrichtenstroms, der in Form von Nachrichtenpaketen übertragen wird, die jeweils einen Paketkopf und ein Nachrichtenteil aufweisen, **dadurch gekennzeichnet**, daß die Paketköpfe unverschlüsselt bleiben und zum Synchronisieren sowie zum Erkennen der Zugehörigkeit eines Nachrichtenpakets zu dem zu verschlüsselnden bzw. entschlüsselnden Nachrichtenstrom dienen und daß der dem Paketkopf eines solchen Nachrichtenpakets folgende Nachrichtenteil verschlüsselt bzw. entschlüsselt wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß mehrere Nachrichtenströme mit verschiedenen Schlüsseln verschlüsselt bzw. entschlüsselt werden und daß der jeweilige Schlüssel durch Auswertung des jeweiligen Paketkopfs ausgewählt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß jeder Nachrichtenteil für sich als Block verschlüsselt bzw. entschlüsselt wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß über die Grenzen eines Nachrichtenteils hinweg verschlüsselt bzw. entschlüsselt wird und daß der Vorgang des Verschlüsselns bzw. Entschlüsselns unterbrochen wird, bis der Anfang des nächsten Nachrichtenteils vorliegt.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß in den Nachrichtenstrom Synchronisationswörter für die Entschlüsselung' eingefügt werden.

6. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß Bestandteile eines Nachrichtenteils, die der Sicherung der Übertragung dienen, dem Paketkopf zugerechnet und nicht verschlüsselt und entschlüsselt werden.

7. Verschlüßler zum Verschlüsseln eines Nachrichtenstroms, der in Form von Nachrichtenpaketen übertragen wird, die jeweils einen Paketkopf und einen Nachrichtenteil aufweisen, dadurch gekennzeichnet, daß der Verschlüßler einen Synchronisationsteil (500) und einen Verschlüsselungsteil (300, 400, 600) aufweist, daß der Synchronisationsteil die Paketköpfe des zu verschlüsselnden Nachrichtenstroms erkennt und den Verschlüsselungsteil darauf synchronisiert und daß der Verschlüsselungsteil jeweils den einem erkannten Paketkopf nachfolgenden Nachrichtenteil verschlüsselt.

8. Entschlüßler zum Entschlüsseln eines Nachrichtenstroms, der in Form von Nachrichtenpaketen übertragen wird, die jeweils einen Paketkopf und einen Nachrichtenteil aufweisen, dadurch gekennzeichnet, daß der Entschlüßler einen Synchronisationsteil (500) und einen Entschlüsselungsteil (700) aufweist, daß der Synchronisationsteil die Paketköpfe des zu entschlüsselnden Nachrichtenstroms erkennt und den Entschlüsselungsteil darauf synchronisiert und daß der Entschlüsselungsteil jeweils den einem erkannten Paketkopf nachfolgenden Nachrichtenteil entschlüsselt.

Hierzu 3 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 195 15 680 A1
Int. Cl.[6]: H 04 L 9/12
Offenlegungstag: 31. Oktober 1996

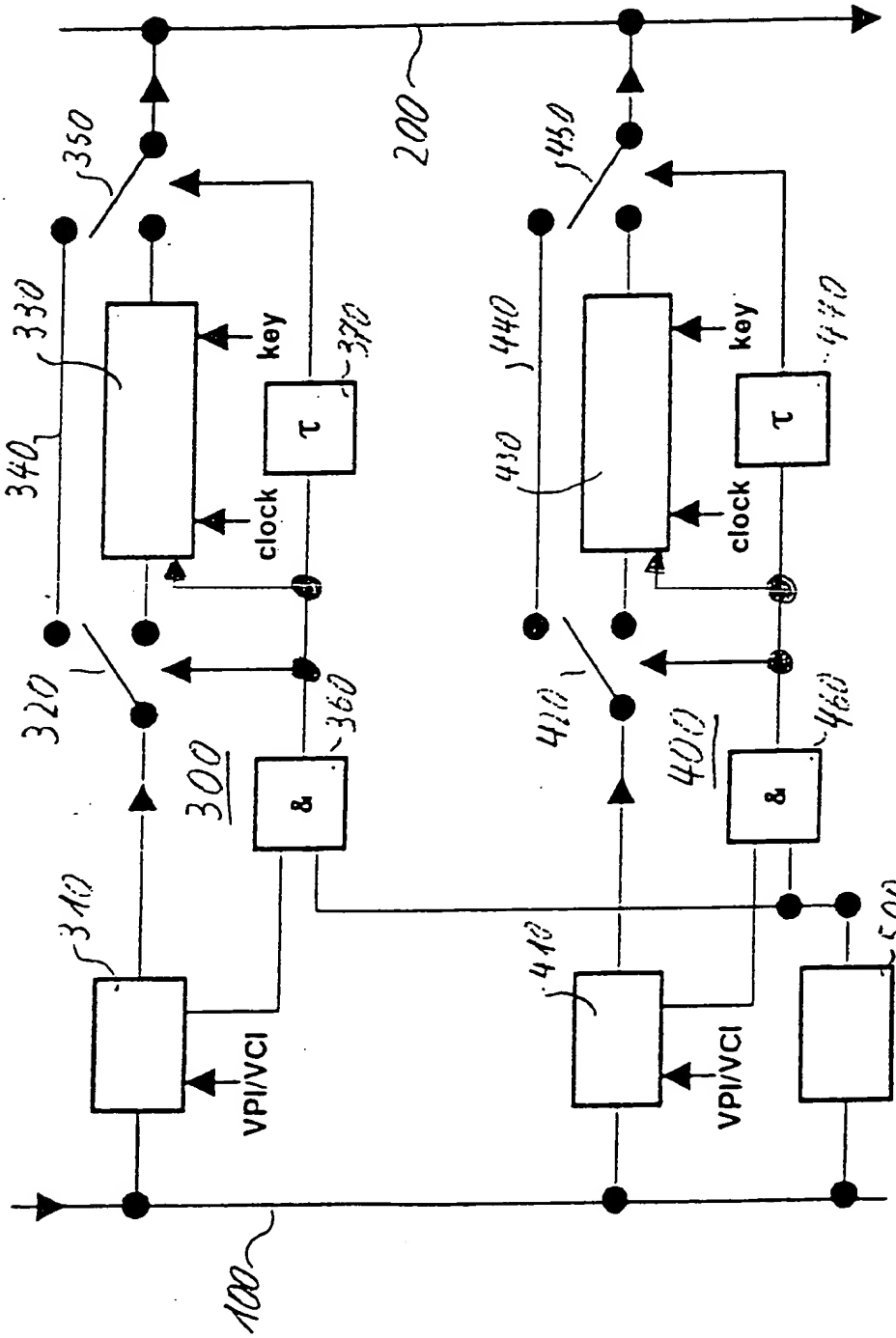


Fig. 1

Nummer: DE 195 15 680 A1
Int. Cl.[6]: H 04 L 9/12
Offenlegungstag: 31. Oktober 1996

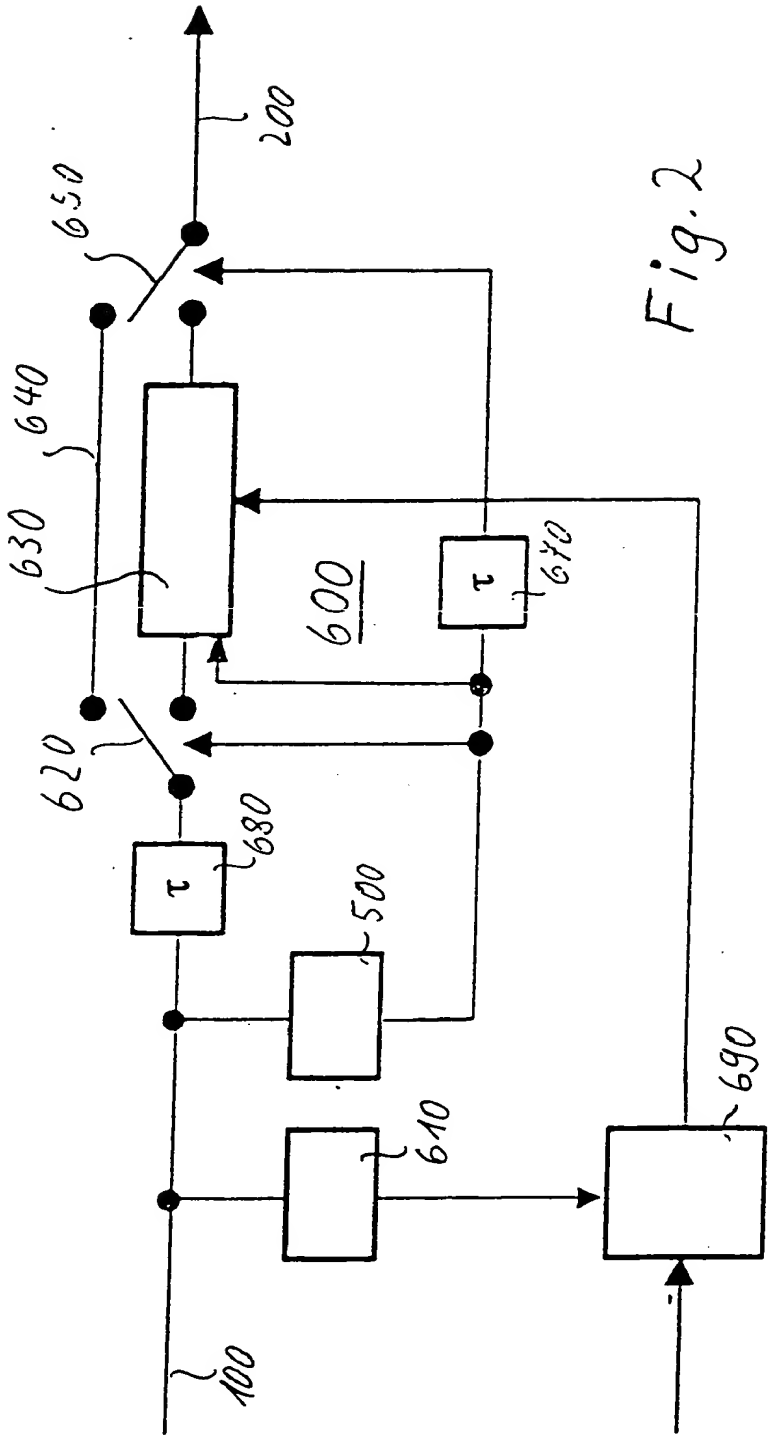


Fig. 2

Nummer: DE 195 15 680 A1
Int. Cl.[6]: H 04 L 9/12
Offenlegungstag: 31. Oktober 1996

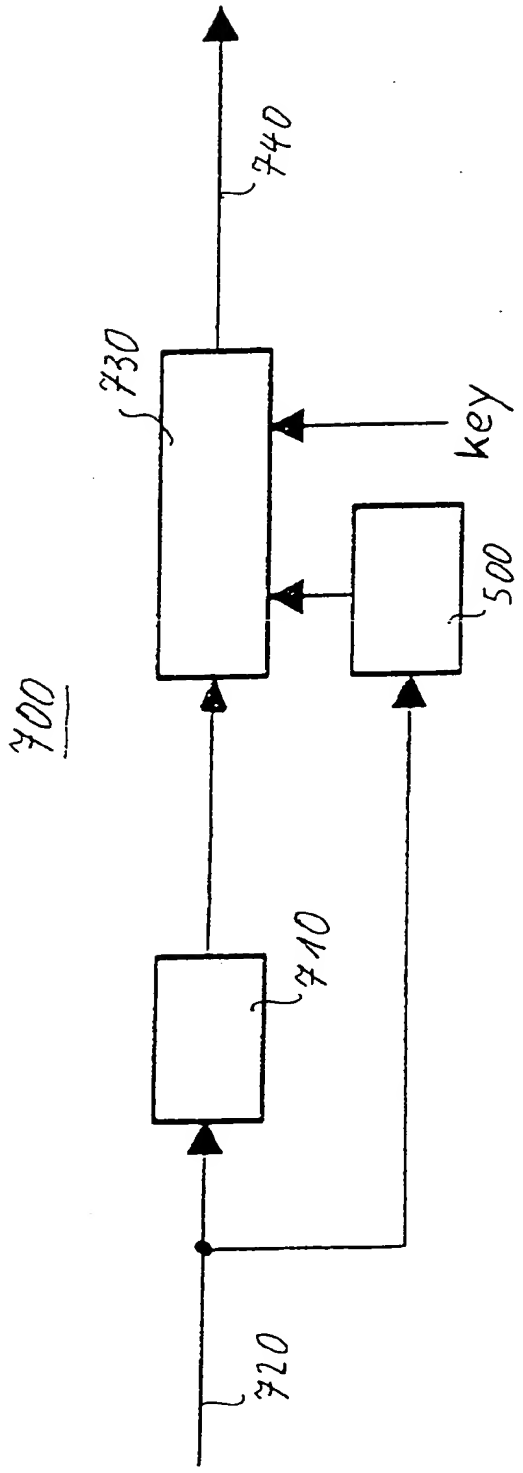


Fig. 2

Encoder and decoder for flow of news in packets

Veröffentlichungsnr. (Sek.)	DE19515680
Veröffentlichungsdatum :	1996-10-31
Erfinder :	BOETTLE DIETRICH DIPL ING (DE); BANNIZA THOMAS-ROLF DIPL ING (DE)
Anmelder ::	SEL ALCATEL AG (DE)
Veröffentlichungsnummer :	DE19515680
Aktenzeichen: (EPIDOS-INPADOC-normiert)	DE19951015680 19950428
Prioritätsaktenzeichen: (EPIDOS-INPADOC-normiert)	DE19951015680 19950428
Klassifikationssymbol (IPC) :	H04L9/12 ; H04L9/16
Klassifikationssymbol (EC) :	H04L9/12, H04Q11/04S2
Korrespondierende Patentschriften	

Bibliographische Daten

The encoder has an input line (100), an output line (200), a first (300) and a second (400) encoding part and a synchronising part (500). Each encoding part includes a filter (310,410), a first switch (320,420), a scrambler (330,430), a bypass line (340,440), a second switch (350,450), an AND gate (360,460) and a delay (370,470). The input data is fed to the filters and the synchronising part, and the filters receive instructions about recognising the flow, while the synchronising part derives a mask for those parts of the flow that have to be encoded.